SE 6000
Security Management System

UNIX-based Host Software and Hardware

A/E Guideform Specification
Version 1.0

Westinghouse
Security Electronics

NOTES:

- The following A/E Guideform Specification conforms to CSI guidelines to provide Specifiers an easy way to include Westinghouse Security Electronics products in their specifications.
- The specifier should carefully select the portions of this document that fit the intended application.
- Feel free to consult with your Westinghouse Security Electronics systems integrator regarding your particular application.
- Optional feature choices are represented by items enclosed in brackets [ ].
- This document is considered accurate through the date on the cover. For updated specifications, call Westinghouse Security Electronics at 408 727-6521
- The following individuals and organizations contributed to this document:

Project team leader/compiler:
- Brent A. Duncan, Marketing Publications Specialist

Core team members:
- Joe Bridgman, Area Sales Manager
- Brian Giampaoli, Area Sales Manager
- Joe Oesterle, US Sales Manager

With contributions by:
- Frank Binzoni, VP Sales & Marketing
- Ken Butte, Project Manager/Readers and Cards
- Bill Blasdell, VP Engineering
- James Collins, Senior Design Engineer
- Dana Frischer, Area Sales Manager
- Tim Hillburn, System Test & Evaluation Manager
- Susan Goldin, Technical Writer
- Peter Keep, Marketing Services Manager
- Steve Lever, Field Service Engineer
- Troy Mickle, Marketing Communications Specialist
- Jim Reeve, Software Engineer
- Alec Ratliff, Field Service Engineer
- Bill Richardson, Technical Instructor
- Ping Saye, Design Engineering Manager
- Tony Smith, Software Engineer
- George Souza, Project Team Director
- Rick Sparks, Project Manager/Controllers
- Matt Wenzel, Field Service Manager

With special thanks to:
- John Suhr, Engineering Director, Tomasi-Dubois & Assoc. Sec. Consultants
- Construction Services Institute

Table of Contents

PART I GENERAL 1
.1 INTRODUCTION 1
A. This document describes the required Electronic Access Control and Security Management System software (Host). 1
B. This specification provides all information necessary to produce a complete proposal for a sophisticated, easy to use multi-tasking, multi-user, UNIX based electronic Security Management System. The appendices contain hardware and software specifications necessary to select the proper equipment for an installation. 1
.2 GENERAL DESCRIPTION 1
A. The required Host shall be a powerful, multi-function security and access management system. 1
B. It shall operate on a high quality Hewlett-Packard (Hewlett Packard) computer running SCO UNIX Operating System. 1
C. Host shall be designed to grow as project needs grow. 1
D. The system shall be simple and economical enough to support a single site, yet powerful enough to manage a continent-wide, multi-site network. 1
E. Modular software shall allow for future system features to be added as management recognizes requirements. 1
F. The system shall employ the UNIX operating system and have true multi-tasking and remote terminal capability. The system provided shall monitor and control independent activities simultaneously at different locations. 1
G. Host shall be designed to control Westinghouse Security Electronics' second-, third-, and fourth-generation security architecture. This architecture currently consists of the 708P, 800 Series, SE 422, NexSentry 4100 Series Controllers, and additional OEM peripheral components. 1
H. Host shall be designed to control, and/or interface with, a variety of OEM peripheral equipment. This equipment shall include, but not be limited to: 1
.3 DESCRIPTION OF WORK 1
A. The Security Management system shall manage the security operations and access control for a single facility or a multiple site network. 1
B. Installing the Security Management system and bringing it to operational status shall require the following major steps: 1
.4 SUBMITTALS 2
A. **Block diagram:** 2
.5 QUALITY ASSURANCE 2
A. **Host Computer:** 2
B. **Manufacturer:** Manufacturer of products defined in this section must have: 2
.6 WARRANTY 2
A. **Systems Integrator:** 2
B. **Manufacturer:** 2
C. **Host System:** 2
D. **Host Software:** Software Maintenance shall include three levels of support, provided by Westinghouse Security Electronics' Customer Service Organizations, via the systems integrator, as follows: 3

PART II PRODUCTS 3
.1 MANUFACTURER 3
A. Westinghouse Security Electronics 5452 Betsy Ross Drive Santa Clara, CA 95054-1102 Telephone: (408) 727-5170 FAX: (408) 727-6707 3
.2 MANUFACTURED UNITS 3
A. The SE 6000 Security Management System product family shall consist of the following: 3
B. The access control and alarm monitoring devices available for Hosts are listed below. For specifications on these products please refer to the corresponding Guideform Specifications: 3
.3 EQUIPMENT 3
A. **General:** 3
B. **Architecture:** 4
C. **Sortware Platform** 5
D. **Operator Interface/Operations:** 6
E. **System Management:** The required system shall perform all of the following functions: 10

F. **Access Control Operation:** The system shall have the capability to control access via either central processing or distributed processing. With central processing, Host or Local/Remote Location Controller shall make all decisions when controlling Westinghouse Security Electronics Access Control Units (Controllers). For distributed processing, an intelligent Westinghouse Security Electronics Controller is required to make all decisions locally. Since the system shall operate differently in these two modes, the following section is divided into three parts, as follows 13
G. **Alarm Monitoring Operation:** 15
H. **Additional Security Operations:** 17
.4 COMPONENT DEFINITION 20
A. Hewlett-Packard computers are required for this system. Seven models may be implemented depending on the nature of the system integrator's design. The four standard platforms designated for the seven models are defined below, each configuration specifying minimum requirements: 20

PART III EXECUTION 23
.1 FIELD QUALITY CONTROL 23
A. **Tests:** 23
B. **Inspection:** 23
C. **Field Service:** 23
D. **On-Site commissioning and/or training:** 24
.2 SCHEDULES 24
A. **System Integrator Assisted Preparation:** 24
B. **System Installation:** 25
C. **Verify Installation:** 25

PART IV APPENDIX ..... A
.1 REMOTE DIAL-UP INTERFACE: MODEL RDI ..... A
A. **SE 6000 Remote Dial-up Interface:** This interface is designed for the SE 800 Series products. ..... A
.2 DATABASE CAPACITIES ..... B
A. **6030/40/50 System Database Capacities:** ..... B
B. **6100 System Database Capacities:** ..... B
C. **6200 Systems Database Capacities:** C
D. **6300 System Database Capacities:** C
E. **LC / RLC System Database Capacities:** ..... D
F. **LC1 / RLC1 System Database Capacities:** ..... D
G. **LC2 / RLC2 System Database Capcities:** ..... D
H. **LC2 / RLC2 System Database Capacities:** ..... D

Page intentionally left blank

PART I GENERAL

.1 INTRODUCTION

A. This document describes the required Electronic Access Control and Security Management System software (Host).

B. This specification provides all information necessary to produce a complete proposal for a sophisticated, easy to use multi-tasking, multi-user, UNIX based electronic Security Management System. The appendices contain hardware and software specifications necessary to select the proper equipment for an installation.

.2 GENERAL DESCRIPTION

A. The required Host shall be a powerful, multi-function security and access management system.

B. It shall operate on a high quality Hewlett-Packard (Hewlett Packard) computer running SCO UNIX Operating System.

C. Host shall be designed to grow as project needs grow.

D. The system shall be simple and economical enough to support a single site, yet powerful enough to manage a continent-wide, multi-site network.

E. Modular software shall allow for future system features to be added as management recognizes requirements.

F. The system shall employ the UNIX operating system and have true multi-tasking and remote terminal capability. The system provided shall monitor and control independent activities simultaneously at different locations.

G. Host shall be designed to control Westinghouse Security Electronics' second-, third-, and fourth-generation security architecture. This architecture currently consists of the 708P, 800 Series, SE 422, NexSentry 4100 Series Controllers, and additional OEM peripheral components.

H. Host shall be designed to control, and/or interface with, a variety of OEM peripheral equipment. This equipment shall include, but not be limited to:

1. Opto 22: non-supervised input/output devices.
2. Stellar: input/output devices.
3. Burle: CCTV equipment.
4. Vicon: CCTV equipment.
5. American Dynamics CCTV equipment.
6. Polaroid ID 4000: image capture & ID badging equipment.
7. Radionics: alarm panels.
8. Recognition Systems: ID-3DR hand geometry readers.

.3 DESCRIPTION OF WORK

A. The Security Management system shall manage the security operations and access control for a single facility or a multiple site network.

B. Installing the Security Management system and bringing it to operational status shall require the following major steps:

1. Determine operational requirements and plan system to implement them.
2. Select Host computer site.
3. Install and integrate Access Control, Alarm Monitoring and related security hardware.

4. Configure Controllers and SE 6000 to communicate with one another.
5. Enter data of security system database.
6. Connect between Host system and Controllers and related hardware.
7. Test security system communications and operation.
8. Train operators.
9. *NOTE: See PART IV.3, "Equipment" for an expansion of this work summary.*

.4 SUBMITTALS

A. **Block diagram:**

1. Submittals shall include a block diagram detailing all connected devices from Host to the door entry device.
2. This document shall be adequate to ensure that all parties involved can determine that the previously defined system meets security system requirements.

.5 QUALITY ASSURANCE

A. **Host Computer:**

1. Host system shall include a Hewlett-Packard Pentium PC serving as Host computer and as multiple Local Controllers.
2. Hewlett Packard XM3 Pentium® PCs may be added as remote terminals if required by the specific configuration. The workstation uses either a 486 EISA or 586 EISA computer approved by the Security Manufacturing Industry for use in industrial security environments.
3. The Host computer shall meet FCC requirements for class B computing devices.

B. **Manufacturer:** Manufacturer of products defined in this section must have:

1. **Industry experience:** Company must have at least 20 years experience in manufacturing and servicing access management systems.
2. **ISO 9001 Certification:** Manufacturing process of company must meet stringent standards of ISO 9001 Certification.

.6 WARRANTY

A. **Systems Integrator:**

1. The systems integrator shall be the first line focal point of all service problems and/or questions directly from the end-user.
2. The systems integrator shall provide direct support for software service issues, hardware problem determination and hardware service repair for the selected system product family.

B. **Manufacturer:**

1. The manufacturers shall provide second line support to the systems integrator for the application and operating software and for the system component and computer hardware through Westinghouse Security Electronics' and Hewlett Packard's respective worldwide service organizations.

C. **Host System:**

1. The Host hardware and software shall be warranted for at least fifteen (15) months from the date of shipment from the factory, or 12 months from the date of installation, whichever occurs first.
2. Exclusive of hardware options, the Hardware Warranty is Hewlett-Packard On-Site Warranty/Service Agreement, with a one day response time, Monday through Friday, 8:00 am to 5:00 p.m.
3. Both Hardware and Software Maintenance shall be included with the system for the first year, at no additional charge.

D. **Host Software:** Software Maintenance shall include three levels of support, provided by Westinghouse Security Electronics' Customer Service Organizations, via the systems integrator, as follows:

1. Phone-in Consulting Service, which provides troubleshooting assistance and answers all functional, procedural and operational questions.
2. On-Line Diagnostic Service, with the ability to remotely dial into a specific system through the modem to diagnose and resolve software problems.
3. On-Line Update Service, which electronically provides updates to the software, via modem. These updates include new revisions of application software, operating software and database management application software, as they are released.

PART II PRODUCTS

.1 MANUFACTURER

A. Westinghouse Security Electronics
5452 Betsy Ross Drive
Santa Clara, CA 95054-1102
Telephone: (408) 727-5170
FAX: (408) 727-6707

.2 MANUFACTURED UNITS

A. The SE 6000 Security Management System product family shall consist of the following:

1. **Host System(s):** Hewlett Packard XM3 Pentium® PCs for ultimate system control.
2. **Local Controller(s):** Hewlett Packard XM3 Pentium® PCs for local control of specific system sub-units.
3. **Remote Location Controller(s):** Hewlett Packard XM3 Pentium® PCs for remote dial-up control of specific system sub-units.
4. **Remote Dial-up Interface(s):** Remote Interface to Westinghouse Security Electronics Alto 818 Series Controllers (Controllers).
5. **Additional Monitors:** Hewlett Packard Monochrome or Color Graphics terminals.
6. **Additional Printers**: Hewlett Packard LaserJet 5 Report, Hewlett Packard LaserJet 5L, Okidata Serial Log, Okidata Parallel.
7. **Access Control / Alarm Monitoring:** SE 708P, SE 800 Series, Alto 818 Series SE 422 Series, NexSentry 4100 Series, Stellar RDU-200.

B. The access control and alarm monitoring devices available for Hosts are listed below. For specifications on these products please refer to the corresponding Guideform Specifications:

1. Westinghouse Security Electronics model 708P Controllers.
2. Westinghouse Security Electronics model 800 Series Controllers.
3. Westinghouse Security Electronics model SE 422 Series Controllers.
4. Westinghouse Security Electronics model NexSentry 4100 Series Controllers.
5. Opto 22 alarm input/output units.
6. Stellar RDU-200 alarm input/output units.
7. Radionics Systems ID 3DR hand geometry readers.

.3 EQUIPMENT

A. **General:**

1. The Security Management System shall consist of multiple functional components and be compatible with the Westinghouse Security Electronics access control hardware connected.
2. The following section describes the required functions and operation of Host.

B. **Architecture:**

1. **Host Computer (Host):**

a. **General:**

1) Host computer shall be the nucleus of the required system. It shall provide all necessary capabilities to manage access and alarm activity.

2) Host shall be the single computer that supports all the functions of Access Control and Alarm Monitoring, including file management, reporting and real-time monitoring / control of security hardware devices.

b. **Local Controller (LC):**

1) In order to provide modular expansion, beyond that required of a Standalone system, the configuration shall include Local Controllers (LC).

2) An LC shall support real time monitoring and control of access and monitoring of alarms, while responsibility for file management and reporting shall remain with Host.

3) An LC shall have the ability to be downloaded with the necessary information about cardholders, access privileges, and alarm processing from Host and to perform its monitoring and control functions independently.

4) The LC shall also store and upload information about access and alarm events when requested by Host in real time via a serial or network connection.

5) While alarm servicing is to be performed on Host, the LC shall monitor the activity in real time using text and/or real time graphic floor plans which show access portals as well as alarm points.

c. **Remote Location Controller (RLC):**

1) A Remote Location Controller (RLC) shall be required in configurations where the need for LC functionality is combined with dial-up communications capabilities of a multi-location network.

2) An RLC shall call Host immediately upon an event occurring which has been defined by the system administrator as an alarm condition such as a door forced open, intrusion, power failure, etc.

3) RLC shall be periodically called by Host to download the necessary information about cardholders, access privileges, and alarm processing plus upload accumulated information about normal access activity.

d. **Remote Dial-up Interface (RDI):**

1) One or more Remote Dial-up Interface(s) (RDI) may be required to allow the integration of remote standalone Westinghouse Security Electronics Controllers into a multi-location network.

2) An RDI shall provide a reliable and efficient interface with a dial-up network, as well as event transaction buffering for not less than 6,000 transactions.

3) RDIs shall integrate remote standalone SE 800 Series controllers into a single Host-controlled network.

4) NOTE: It shall be the responsibility of the Authorized Westinghouse Security Electronics dealer, or system integrator, to determine and recommend the optimum arrangement of host and associated computers and peripherals to satisfy the design requirements unless they are specifically stated in the text of this specification. Multiple design configurations may be considered.

e. **System Redundancy:** The SE 6000 shall have the capability to provide three solutions to the requirement for redundant/back-up systems. These approaches to redundancy shall consist of:

1) **Stand-by System:**

(i) This level of redundancy shall provide a second CPU which shall be easily accessible, but not connected, to the primary system.

(ii) In the event of failure the Stand-by System shall include an Hewlett Packard XM3 PC of the same capability as Host, with processor, hard drive, tape drive, SVGA video board, standard memory, additional memory, corollary board, host bus adapter if required for the specified configuration, and all essential software to operate the system.

(iii) This system shall replace a failed Host CPU, shall have all necessary system applications loaded, and shall be activated by connection to the proprietary security key device utilized with Host system.

(iv) The Redundant Stand-By System shall only be activated only in the event of hardware failure at the Primary System.

2) **Host/LC:**

(i) The second level of redundancy is available through the standard architectural design of the SE 6000.

(ii) In the event of a failure of the LC computer, Host / LC design shall be implemented through the configuration of Host to accommodate manual switchover to the LC computer.

(iii) At the time of switchover the pollers shall be activated through Host rather than through the LC. Host would then function as the LC for monitoring purposes until the LC was again functional.

(iv) If a Host failure is experienced, the LC would continue to perform in its usual manner.

3) **Fault Resistent System (FRS):**

(i) This level of redundancy shall support simultaneous reads and writes to two disks of two duplicate platforms configured identically.

(ii) Under normal conditions the Primary Host would be the main functioning system writing all transactions to the disk of the Secondary system in real-time.

(iii) In the event of Primary Host failure, the FRS CPU will automatically seize control of the entire system until the Primary Host is restored and control returned to the Primary Host.

C. **Sortware Platform**

1. **Operating System:** SCO UNIX.

2. **Database Management System:**

a. System shall utilize a high-performance relational database management system such as UNIFY Accell/SQL.

b. The system shall be capable of multi-user and multi-database support in a UNIX environment.

3. **Advanced Visual Report Writer:**

a. The system shall utilize a powerful visual information and retrieval tool to extend the reporting power of UNIFY Accell SQL application development system.

b. The retrieval tool shall work seamlessly with Accell SQL to provide rapid generation of custom reports and business graphics.

4. **Screen Interface System** (on Ethernet only)**:**

a. X-windows capabilities shall be provided to support File Maintenance, Reporting, Monitor and Graphics Windows.

b. These functions shall be available on the PC Terminals connected to the system, and shall incorporate X-Windows software.

5. **Networking:**

a. Networking capability shall be necessary to implement large scale and/or multi-location systems with security devices and/or computers distributed to remote locations while overall control of the network is maintained at a central location. Local Area Networks (LANs) or Wide Area Networks (WANs) connected via dedicated or dial up communications lines may be required.

6. **"C" Programming Language:**

a. The application shall be written in the "C" programming language.

b. This standardization shall provide for greater ability to support and enhance the system in the future.

D. **Operator Interface/Operations:**

1. **Sophisticated Operator Interface:** The required system shall provide a sophisticated, easy to operate interface for security operators. The following aspects of the system shall contribute to the effectiveness of the operator interface:

   a. **Graphical user interface:**

      1) A graphical user interface, based on the X-Windows system, which permits a user to view and operate multiple screens in several areas of the system simultaneously.

      2) The operator shall have the capability to customize the individual screen sizes and locations, in relationship one to the other, on the display.

   b. **Menu driven operation:**

      1) Menu driven screen selection shall allow even an infrequent operator to move through and manage the functions of the system easily and with a minimum of training.

      2) There shall be no need to memorize complicated commands or procedures.

   c. **Function keys:**

      1) Function key control of actions must provide the ability to control the system with simple keystrokes.

   d. **Windowing:**

      1) The system shall provide windowing (a ZOOM feature) for additional information and/or explanation.

      2) The ZOOM capability shall allow the operator to look up information in supporting files, and to access other screens without leaving the screen they are presently using. For example, while entering data for a cardholder, the operator may require auxiliary information regarding access codes. The operator may ZOOM to the access code screen, key on the correct information and dynamically add that data to the Keyholder Entry screen.

      3) All this shall be accomplished without having to exit one screen, move through the menus, enter another screen to retrieve the necessary information, then move back through the menus in order to make the entry in the original location.

      4) This feature shall exist throughout the system, wherever categorical descriptions are kept in lists.

2. **Multi-Terminal and Multi-Tasking:**

   a. **General:**

      1) Multi-Terminal operation for interaction by additional operators shall be available at local or remote sites.

      2) Independent operations may be performed at different operator terminals with minimal degradation of performance.

   b. **Terminals supported:**

      1) The system shall be able to support up to: [4 terminals (SE 60XX)] [4 terminals (SE 6100)] [8 terminals (SE 6200)] [12 terminals (SE 6300)] in any combination of monochrome and SVGA color PC terminals.

      2) Maximum additional terminal configurations require additional memory.

   c. **Connection:**

      1) Additional terminals shall either be directly connected to Host system via a serial link or network connection or shall available on a dial-up line.

      2) In any of the available configurations, additional terminals shall have the same capabilities as the main console.

      3) Operations at any terminal shall be limited by operator name and password (refer to “System Password Protection/Control” section below).

d. **Routing Alarm Reports:**

1) The system shall have the ability to provide the routing of alarms and alarm instructions to more than one CRT or printer, dependent upon end-user customization requirements.

2) This routing capability shall include categorizing alarms based on “zones” (physical grouping) and “tenants” (people grouping) and then assigning “zone” and “tenant” responsibility to specific monitoring stations and personnel.

e. **Routing of Alarms by Tenant:**

1) The system shall allow for a certain sub-set of cardholders, doors, and alarm points to be assigned to one tenant.

2) A tenant is defined as having exclusive access to a specific set of cardholders, doors and alarm points located within a pre-defined geographic area. This definition is in keeping with the system capability which enables multiple, separate companies to share the same global information on a single system, while at the same time, maintaining specific proprietary information as necessary for each company.

3) Any operator for a single tenant shall receive alarms and access activity exclusive to their respective part of the system, and invisible to other system tenants. These alarms and transactions shall be distributed based on operator's password and authorization level rather than the terminal being used.

3. **System Password Protection/Program Security Levels:**

a. Access to all menus and screens, and the corresponding capability for each screen, shall be controlled via operator and password authorization levels.

b. Accessibility to the over 160 individual screens shall be defined on an individual basis by the System Administrator to limit a system user to specific screens and functions.

c. Additional authorization protection shall be provided by means of defining, on a screen by screen basis, whether a user is granted permission to View, Add, Delete or Modify the information on that particular screen or perform control functions such as Lock/Unlock doors, Shunt/Unshunt alarms, etc. This added level of control shall serve to protect the system and prevent unauthorized changes to information which could compromise the data integrity and the system security.

d. Not less than 1,000 operators shall be allowed, each with a completely unique set of individually defined capabilities.

4. **Real Time Alarm Reporting and Display:**

a. The system shall process alarms in real-time, using not less than 10 priority levels defined by the System Administrator. The System Administrator shall have the capability to assign the priority levels into categories such as fire, intrusion or duress.

b. Alarm displays shall be in color. The system shall have the ability to assign unique colors for different alarm priority levels.

c. Unacknowledged alarm messages shall be repeated after a user-defined time period.

d. The system shall associate color graphic maps with alarm points and shall display maps in real-time. Graphic maps shall update automatically and shall not require a “Refresh” command.

5. **Real-time Status Reports:**

a. System status reports shall be available by alarm category, security area device and monitor points.

6. **Override Command Capability:**

a. The system shall provide the operator the ability, based on previously defined password authorization, to override pre-set conditions.

b. The overrides shall include:

1) Unlock / Relock doors.

2) Shunt / Unshunt alarm monitor points.

3) Open. Limit and/or Close the areas covered by specific Controllers.

4) Forgive anti-passback status in individual Controllers.

5) Shunt, unshunt and restart Controllers.

6) Halt and restart pollers.

7) Activate/Deactivate project schedules.

8) Activate/Deactivate relay outputs.

7. **High Resolution Color Graphics at Operator Console:**

   a. SVGA resolution with 256 colors minimum.

   b. Vector resolution for maps:

      1) Utilizing a mouse to facilitate the selection and placement of graphic symbols, the system shall define maps representative of the site. The symbols shall be associated with alarm points.

      2) Mapping shall support a "Jump" function which shall allow definition of maps of a lower level detail than the map currently displayed.

      3) The mapping system shall support output to the following printers:
         (i) Hewlett Packard LaserJet 5.
         (ii) Hewlett Packard LaserJet 5L.
         (iii) Okidata Serial Log.
         (iv) Okidata Parallel Log.

8. **Powerful System Diagnostic Software:** This feature shall provide operators with greater ability to examine the status of the system components and communications. These capabilities are particularly useful to diagnose suspected problems.

   a. **Card Reader Status:**

      1) A status screen shall show the condition of all card readers attached to the system.

      2) This screen shall show the status of card readers, coax cables.

   b. **Card Reader Activity:**

      1) Access activity at doors associated with a particular card reader shall be displayed as it occurs.

      2) Information displayed shall include the following:
         (i) Door name.
         (ii) Access time.
         (iii) Card number/PIN.
         (iv) Door status: closed, open, held open or forced open.
         (v) Keyholder Name.
         (vi) ID number.
         (vii) Lock status: locked, unlocked, manually unlocked or auto unlocked.
         (viii) Monitor Point Status: Active, clear, communications failur, device failure.

   c. **Communications Monitor:**

      1) Communications between the card readers and the computer must be monitored. This function shall be used during installation to verify proper connection of communication cables, and during standard system operations to monitor the status of device connections.

9. **High Security Mode and Complete Audit Trail:**

   a. This feature shall be implemented to provide a complete history of data changes to the system, by documenting all changes to the database, excluding system generated transactions or logs.

   b. The information to be tracked shall include the user making the change, the data that was changed, and the date the change occurred.

c. The Audit Trail implementation shall include reporting on the information that affects keyholder access and alarm events, including the following files:

1) Keys holders.

2) Pollers.

3) Devices.

4) Readers.

5) Points.

6) Holidays.

7) Access Groups.

8) Access Codes.

9) Employee Access Assignments.

10) Time Codes.

11) Instructions.

12) Auto Opens/Activates.

13) Device Reports PIN Definition

14) PIN Hardware Definition.

15) Dialers.

16) All SQL database items.

d. The audits for these files shall be stored in an independent flat file resident outside of the database.

e. The audit trails shall contain all fields of the affected record, not just the field that was changed. in order to provide a "before and after" image of the data.

f. The File Maintenance programs of each of the affected files shall be modified to log the audit records to the flat file.

g. A report shall be provided for each of the audit files, and shall print all of the fields of the audit record in addition to the date and time of change, the log-in name of the user making the change, a serial number identifying the line of audit, and whether the change was a modify, add or delete.

h. Each Audit file shall be able to be archived to tape. Once the audit record is successfully written to tape, the on-line audit record shall be deleted.

10. **Event and Task Programming:**

a. Custom programming, to define a set of tasks to be performed as the result of a specific event, shall be achieved through the Event and Task programming option.

b. Events such as an access event, alarm condition, or timer may be linked to an output. The capability for this level of customization is standard on the SE 6000 system.

c. The creation and implementation of special Event / Task relationships depend upon careful definition of customized transactions under a resident program facility.

d. One Event is capable of driving one, or multiple, Tasks.

e. Event / Task would be implemented to activate certain alarms or indicators any time a specific event took place at a critical point in the facility.

f. Example: If a Command Key which is not valid is presented at a critical door, a special alarm message can be programmed to appear at the monitor screen while, simultaneously, lights and audible alarms are activated at the site of attempted entry.

11. **Project Schedules:**

    a. Implement the capability to use project schedules to alter access to certain doors by activating and de-activating "projects" in the SE 6000. This functionality shall work with access codes and privilege levels to provide another level of clearance checking to the system.

    b. **Doors per project:** 16 maximum. Doors included in an active project can be accessed only by cardholders who are assigned a project that includes that door.

    c. **Projects:** 128 maximum. The system shall provide the capability to define, modify, add and delete projects.

    d. **Access Override:**

        1) Implementation of an Access Override feature shall enable one to quickly turn on and off access, manually or by date, to particular sites of a facility.

        2) This feature shall incorporate Access Override Codes (AOC), each of which may be given a description, a range of dates, and whether access shall be allowed or denied during the range of dates.

        3) Subsequently, these codes may be assigned to one or more of the access privileges assigned to each keyholder. Therefore, each cardholder's individual Access Code, or Group Records may be assigned an Access Override Code. As a result, in addition to controlling access by door, time of day, and day of week, access privileges may also be controlled by date.

    e. The system shall not only check access by door, time and day, it shall check to see if access has been limited to a range of dates, and whether access should be allowed or denied through that range of dates. This method of implementation shall, therefore contain several properties, as follows:

        1) Identical Access may be assigned to a group of cardholders, but restrictions may be applied to a subset of cardholders.

        2) Identical Access may be assigned to a group of cardholders, but restrictions may be applied differently.

        3) Different Access may be assigned, subject to the same date restrictions.

    f. Keyholders whose Access Privilege Records have not been assigned an Access Override Code shall be unaffected by this feature. This feature shall be functional for Host decisions.

E. **System Management:** The required system shall perform all of the following functions:

1. **Simple System Administration:**

    a. To administer Host computer, the system shall provide control of all system administration functions via menu accessed screens.

    b. There shall be no need to memorize complicated commands or to learn the syntax of the UNIX operating system.

    c. System administrative functions shall include:

        1) Adding and deleting system users.

        2) Maintaining user passwords.

        3) Checking database statistics.

        4) Performing system and database backups.

        5) Defining and maintaining program security levels.

        6) Displaying current system activity.

        7) Performing transaction archives.

        8) Initiating data transfer to remote devices.

        9) Defining and maintaining user-controlled fields.

        10) Performing alarm transaction clean-up.

        11) Displaying those users currently logged on the system.

        12) Key holder loading.

13) ID Security maintenance.

2. **Security System Hardware Definition:**

   a. The capability to define the system hardware to the following degree shall be allowed:

      1) Access control/alarm monitoring devices.

      2) Communications characteristics.

      3) Grouping by zone and tenant.

      4) Grouping by Anti-passback levels.

      5) Defining readers.

      6) Defining points.

      7) Defining CONTROLLER reports.

      8) Defining auto activate/open periods:
         (i) Proximity access control.
         (ii) Magnetic card access control.
         (iii) Keypad access control.
         (iv) Alarm monitor points.

3. **Define Security System Software**: The system shall allow for the specific definition of system software in the following areas:

   a. **Keyholder information:**

      1) The system shall be capable of keyholder information entry independent of the assignment of card numbers. It shall also have the capability to assign each keyholder to multiple access groups.

      2) In central processing mode, the number of possible access groups shall be not less than 100.

      3) Keyholder information shall include the following:
         (i) ID number.
         (ii) Card number.
         (iii) Personal Identification Number (PIN)
         (iv) Employee name.
         (v) Tenant.
         (vi) Card valid date.
         (vii) Card expiration date.
         (viii) Six user-definable sort fields with field look-up (ZOOM) capability.
         (ix) Seven text-based data entry field.
         (x) Address, telephone number and other applicable fields.

   b. **Time periods:**

      1) Time periods shall include:
         (i) Start time.
         (ii) Stop time.
         (iii) One or more days of the week.

   c. **Holidays:**

      1) In addition to the time zones, days of week and doors for access, the system shall allow the System Administrator to add holidays to the access definition.

      2) Holiday definition allows days defined as holidays to have automatic and access parameters different from their normal definitions.

d. **Zones:**

1) The system shall have the capability of dividing the physical site into zones for anti-passback control and for arm/disarming security functions.

2) Zone definitions shall be applied to card readers into or out of the zone.

e. **Tenancy:**

1) The system shall allow for security hardware, areas, and cardholders to be grouped as tenants in the case of multiple tenant occupied facilities.

2) An operator assigned to a particular tenant group can manage data, acknowledge alarms or execute reports only for data and events defined for that tenant group.

4. **Maximum Database Capabilities:**

a. Maximum storage capabilities are dependent on Host and Controller configurations selected.

b. Refer to Appendix B for database requirements.

5. **Database Download to Distributed Local Controllers:**

a. In situations where Controllers with distributed intelligence are connected to the system, Host must download all information pertinent to that particular control unit.

b. The system shall execute downloads automatically when data is added or changed, or by manual initiation.

6. **Powerful and Meaningful Reports:** System shall have the following reporting capabilities:

a. System shall offer rapid generation of custom reports and business graphics, through time-saving features such as visual report writing; batch reporting; and database, output, arithmetic, selection and sorting functions.

b. System shall provide a simple, logical tool for producing custom reports without programmer assistance, without compromising the security and integrity of the DBMS.

c. System shall be able to execute reports without intervening with, or impacting the performance of, the real-time operation of the security system.

d. System shall track and report the dates of archived events available for reporting. It shall have the capability to generate reports for activity spanning any time period through the use of disk files, tape archives or a combination of both forms of media.

e. System shall separate reports by tenant, when defined, so that an operator assigned to a particular tenant group shall be inhibited from accessing data and reports on areas of the security system from outside the defined tenant group.

f. System shall provide reports for every data file maintained in the system. These reports provide for data entry verification and printed back-up.

g. Reports may be customized to any reporting format desired from an unlimited number of files or tables, and select, sort and perform calculations on any fields in those files.

h. The system shall provide Unify ACCELL DBMS for data storage and manipulation. Unify ACCELL DBMS is a relational database manager which supports SQL, the electronic industry standard for interfacing with sophisticated data management systems. The system shall also employ a tool for customized report generation.

7. **On-Line Storage of Security Events:**

a. Minimum on-line log transactions: 100,000 on a low-end system (SE 60XX); 400,000 to 2,000,000 on a high-end system (SE 6300).

8. **Archiving of Security Events:**

a. The system shall provide the ability to backup to streaming tape all events stored in the transaction file through a user-selected date.

b. Reports shall be generated from the archived data.

9. **Backup and Restoration of Security System Definitions**:

   a. The system shall provide the capability to backup to streaming tape the security system definition, including both hardware and user information.

   b. System back-up shall be initiated by a menu option for optimal simplicity.

   c. In the event of data corruption, tampering, or other loss of data integrity, the security system definitions shall be capable of being restored to the on-line system from the backup tape.

   d. Database back-up functions shall be transparent to the system administrator and to the system functionality. Back-up of the SE 6000 database and transaction logs does not require the system to be shut down. Operator interaction, such as monitoring, file maintenance and database entry, shall continue in an uninterrupted state during the process of archiving.

   e. The system shall provide capability for a complete back-up of the system via the user interface, with an accompanying restore ability. The back-up function, presented as a menu option, offers the choice of either a complete system back-up or a database-only back-up. This functionality also keeps track of the last date of each type of back-up for historical reference. Additionally, the application employs a dedicated user log-in to facilitate the recovery of database back-up tapes, providing a faster, easier, more efficient method of restoring a database.

F. **Access Control Operation:** The system shall have the capability to control access via either central processing or distributed processing. With central processing, Host or Local/Remote Location Controller shall make all decisions when controlling Westinghouse Security Electronics Access Control Units (Controllers). For distributed processing, an intelligent Westinghouse Security Electronics Controller is required to make all decisions locally. Since the system shall operate differently in these two modes, the following section is divided into three parts, as follows

   1. **Common Requirements** (both Central and Distributed Processing):

      a. **Expanded Growth Capacity:**

         1) Through new Host systems, additional controllers, and computer hardware upgrades, the system shall provide support for large scale systems with an extremely large number of cardholders, card readers, alarm points, operator terminals, or transaction events. This unlimited expansion capability shall provide a secure foundation for future growth and, also retain the investment in the initial system components.

         2) Modular software architecture and performance-oriented programming techniques shall optimize the system to provide minimum response time. From the speed with which doors are unlocked, and the speed with which reports are produced, the system software must be able to meet the stringent specification for capacity as listed in Appendix B.

      b. **Expanded Network Support:**

         1) The system shall have the capability to implement large scale or multi-location systems with security devices or computers distributed to remote locations while maintaining overall control of the network at a central location. Systems may use Local Area Networks (LANs) or Wide Area Networks (WANs) connected via dedicated or dial-up communications lines.

      c. **Event Capture from Access Control Units** (Controllers):

         1) Host computer shall receive and record all events that occur at all Local Controllers.

         2) Event capture shall occur either real-time (to hard-wired devices) or when required (to dial-up connected devices). These devices may include Local Controllers, Remote Location Controllers, Remote Dial-up Interfaces, Controllers, and alarm monitor units.

      d. **Dial-up Reporting from Controllers:**

         1) When alarms or other priority events occur, Remote Location Controllers or Controllers connected via dial-up lines shall call Host computer to report the event.

      e. **Failsoft Operation:**

         1) If for any reason, communications between the computer and the Controller is interrupted, the system shall resume control upon restoration of communication.

         2) While connected to Host, the system shall constantly update the Controllers with the information necessary to operate in failsoft mode.

f. **Automated System Control:**

1) The system shall provide the ability to automatically change the state of certain devices and/or areas based on time.

g. **Multiple Identification Required for Access:**

1) Selected entrances and exits require multiple methods of confirming identity for entry.

2) The required system must support any combination of the following access controlling devices:

(i) Proximity card readers.

(ii) Magnetic stripe card readers.

(iii) PIN keypad.

(iv) Biometrics (hand geometry readers).

h. [**Electronic Visitor Directory:**

1) The visitor access control system (Electronic Visitor Directory) shall provide the ability to track visitors who are not issued an access card.

2) The operator may enter a visitor ID number and the employee ID number of the person they are visiting. A quick look up must be provided for visitors by last name and all visitor records shall be saved for future reference.

3) The optional capability must exist to print a visitor's badge with the valid date and person being visited. The badge must be able to be printed in different colors representing the day of the week.

4) When the system prints a badge, it shall also provide a permanent log of every visitor and the person the visitor is seeing.

5) NOTE: The specifier should carefully select the portions of this section that fit the intended application. Particular attention should be paid to employ only the text for the processing (Central or Distributed) and corresponding Controllers that match the end user's requirements. The presence of any existing Westinghouse Security Electronics Controllers (708P, 800 Series or SE 422) should be carefully considered in determining the ultimate nature of the system.

6) If central processing is to be used, select the features desired for your system from the list of features defined in PARTII.3.F.2 Central Processing below. Budgetary considerations are very important in selecting these features since many of them require additional hardware and/or software. Consult Westinghouse Security Electronics, or your local Authorized Dealer, for application configuration assistance and local contact information.]

2. **Central Processing:**

a. Systems with large numbers of cardholders or access groups, high security environments requiring anti-passback, two-man rule, access decisions based on multiple events (such as card presentation, PIN entry, biometric identification, or display of a cardholder's photo) shall require central processing.

b. Central processing shall be dictated in situations where loss of communications between a Controller and Host computer is considered a potential attack on the system and, as a result, the access privileges must be minimized until appropriate personnel have been notified and communication restored.

c. **Smart Failsoft Operation:**

1) If for any reason communications between the Host and the Controller is interrupted, the Controller shall recognize that event and shall automatically begin operation in a stand alone mode based on predetermined access control criterial.

2) When communication is restored, the system will resume control and receive all stored transactions.

d. **Anti-passback:**

1) **Zoned anti-passback:** The system shall provide zoned anti-passback, which requires users to alternate the presentation of cards to entrance and exit readers.

2) **Assigning passback zones:** The system shall be able to assign a passback zone and a direction (in or out) to each card reader. A data log shall be generated, and passage denied, when there is failure to alternate entry and exit. The system shall be able to assign a zone number for an adjacent zone number; for example, the system can define a single card reader entering zone 1 and exiting zone 2.

3) **Passback forgiveness:** Ability to forgive passback status shall be available via operator overrides. Passback forgiveness shall be provided to a single cardholder or for all cardholders. In the event of system failure, the system must automatically forgive all passback status upon return to an operational state.

4) **Concentric security areas:** must also be definable by the system administrator.

e. **Trace:**

1) The system shall provide the capability to trace activity for specific cardholders at specific doors.

2) The system shall issue a report whenever a cardholder marked for "Trace" is presented at any door.

3) For a cardholder the system shall report activities throughout the system. The system shall display trace activities with the alarm functions to alert the operator.

4) Whether access is being traced or not, the system shall store the last 20 (twenty) access attempts, even after archiving of logs to tape.

f. [**Two Man Rule/ Escort Required Access:** (optional module)

1) This application shall provide the capability for the system to require an access request by more than one person before access is granted into a controlled area.

2) Access shall not be granted unless two individuals with valid access privileges present their keys within a predetermined period of time. The system shall be able to assign this capability to any door.

3) Additional individuals may enter the area after the first two have entered. However, at no time may fewer than two people remain in the room. Thus, if two people are in the room, and one decides to exit, the system shall NOT grant access to exit unless the second person also presents a card for exit access.]

3. **Distributed Processing:**

a. Distributed processing decision making is supported by all WSE Controllers. These intelligent controllers make access decisions at the peripheral device, or door level, independent of Host computer unless the card number is not in the memory of the Controller, or has been modified as a Host controlled card via the Smart Failsafe feature. In that case, Host shall check access privileges and, if access is permitted, shall command the Controller to open the door within 1 second or less when interfaced with a Westinghouse Security Electronics' front end security system.

b. **Automated Download of Data to Distributed Controllers:**

1) SE 6000 maintains a central database on all access control equipment. The database includes cardholders, access levels, automatic events (such as auto unlock), etc.

2) Database sorts this information and sends it to the appropriate intelligent Controller, allowing the local Controller to make all necessary decisions without the SE 6000 Host support.

G. **Alarm Monitoring Operation:**

1. **General:**

a. The system shall provide full Alarm Monitoring and Acknowledgment functionality on both Host computer and the Local Controller (LC) for ease in maintaining data integrity and in the event that communications between Host and the LC is lost.

b. The system shall also provide automatic uploading of alarm acknowledgment data from the LC to Host.

c. Automatic transfer of map data entered on Host, in addition to the ability to display and print maps, shall be available at the LC.

d. *NOTE: System requirements may include some or all of the following alarm monitoring standards. The specifier should carefully select the portions of this section that fit the intended application.*

2. **Line Supervision / Response Time:**

   a. Host, LC or RLC shall interrogate each alarm point at a minimum of twice per second.

   b. When utilizing WSE Controllers, Host system shall monitor the alarm points in two states: secure or alarm.

   c. An end-of-line resistor indicates the point is secure.

   d. Host optionally may communicate with input points via Opto 22 and Stellar alarm input/output units.

3. **Configurable Alarm Instructions:**

   a. The system shall provide the capability to assign up to eight (8) lines of forty (40) characters each for each alarm or monitor point in the system.

   b. The system shall have the capability to assign alarm instructions to monitor points in the system for unique responses to any circumstance.

4. **Operator Alarm Response:**

   a. When acknowledging an alarm, the operator shall have the capability to enter up to eight (8) lines of forty (40) characters each in describing actions taken regarding this alarm event.

   b. User definable fields which contain specific instructions for operator alarm acknowledgment shall be available to the operator, and access to them controlled via pre-defined security levels.

   c. The system shall save alarm acknowledgment with the respective event for future recall and reference.

5. **Recall Alarm Activity:**

   a. The system shall save to disk information associated with each alarm that occurred within the system.

   b. The corresponding alarm instructions and any comments an operator made when acknowledging the alarm shall also be saved to disk. The operator shall not be able to modify or delete this information. Hence, all information is available to the operator viewing an alarm.

6. **Alarm Conditions:** 100 minimum.

7. **Monitor Point Status Display:**

   a. The system shall provide a display that summarizes the current condition of all (or a portion) of the monitor points.

   b. The status display shall indicate normal, active, shunted and communication line status.

8. **Shunting / Unshunting Alarms and Alarm Points:**

   a. The system shall provide the capability to shunt and unshunt alarm points via the following methods:

      1) Automatically: based on time of day, day of week or holiday.

      2) Manually by operator override: The operator must previously have been provided the capability of shunt/unshunt via the password definition.

      3) Status of another point can determine whether a point is active or shunted.

      4) Card Presentation or PIN entry: This allows a group of readers or keypads to be combined to shunt/unshunt alarms within that area.

9. **Operator Definable Alarm Task Programming:**

   a. Tasks available: 100 per event minimum.

   b. The operator shall be provided with the capability to define a set of tasks to be performed by the system as a result of a specific action. For example, an event such as an alarm condition (smoke detector activated), access event (invalid access attempt) or time trigger (60 seconds after a duress button was pressed) shall initiate a task or series of tasks.

   c. The tasks performed may consist of activation of an output relay and/or control commands sent to a CCTV switcher.

H. **Additional Security Operations:**

1. [**Elevator Control** (optional module on SE 60xx):

   a. **General:**

      1) Elevator Control shall be provided via software which provides complete floor by floor access control for elevator cars by allowing activation of only those buttons which control floor access as defined for each specific cardholder.

      2) Elevator Control shall operate without dependence upon any particular elevator panel, thus allowing interface with virtually any commercial elevator operating system.

   b. **Elevator Control capabilities include:**

      1) Floor by Floor Cardholder Access Control:
         (i) As a card is presented to a reader installed within the elevator car, dependent upon the access privileges previously defined, specific floor buttons are enabled to allow specific floor access.
         (ii) The floor buttons remain enabled for a user-definable length of time before automatically defaulting to the deactivated mode.

      2) **Multiple Hardware Support for Output Control:**
         (i) The Elevator Control program shall interface with WSE Controllers, and Opto 22 input/output multiplexor devices to control the enabling and disabling of elevator buttons.

      3) **Controllable Fail-soft Operation:**
         (i) In conjunction with Opto 22 multiplexor boards controlling output contacts, the Elevator Control option shall provide for the programming of the elevator button profile in the event of lost communications with Host computer.
         (ii) This form of watchdog operation provides the capability of enabling specific buttons, as required, during a communications failure.

      4) The Elevator Control software shall be included as part of the basic application on a high end (SE 6100, 6200, 6300) system.]

2. [**CCTV Control** (optional module):

   a. **General:**

      1) Closed Circuit Television communication interface shall enable the system to monitor and control specific elements of a CCTV system through the security management system.

   b. **Functions:**

      1) Camera/Monitor Control:
         (i) Manual selection of the camera scene for viewing on CCTV monitors from Host, thus eliminating the requirement for remote switcher control.
         (ii) Response to system events shall be provided to allow the assignment of a specific camera scene to a specific monitor at the occurrence of a pre-defined alarm condition. When camera sequencing is enabled, the system shall provide the capability to halt the sequencing and display the requested camera scene at a specific monitor. Sequencing shall then be re-initiated at the discretion of the operator.
         (iii) Preset camera and monitor control shall be provided to preset the pan, tilt, zoom and focus for optimum view of a particular area or location.

c. **System Information Entry:**

1) The system shall allow for the programming of camera titles at any camera or alarm location that is part of the automatic sequence, or is selected manually.

2) The system shall allow for the display of the date and time at the CCTV control monitors.]

3. [**SE 6000 Integrated ID System (IDS):** (optional module)

a. **General:**

1) The system shall interface with an Image Capture module that provides the capability to capture and store photographs of cardholders, and transfer those digital photographs to the access control database in order to be retrieved and displayed on a terminal screen for visual verification of identification.

2) The System shall utilize a Windows® based image creation environment which shall provide a single integrated database to eliminate redundant data entry.

3) Alphanumeric text shall be incorporated into the information printed on both the badge and CRT display.]

4) Systems requiring synchronization of two or more databases will not be accepted.

b. **Image Storage:** 15,000 minimum.

c. **Image Recall:** by command, alarm event or card reader transaction logs.

d. **Media Options:**

1) Thermal.

2) PVC: PVC media must be capable of direct-to-card printing on both sides of the card with the ability to hole punch for either horizontal or vertical display.

3) The system shall support both color and black & white images, and have the capability for simultaneous access on multiple terminals.]

4. [**Guard Tour Monitoring** (optional module):

a. **General:** The Guard Tour option shall have the capability to:

1) Define, schedule, monitor and report the status of guard tours.

2) Define the route, timing and locations.

3) Schedule, monitor, cancel and resume tours.

4) Provide printed reports on tour activity and history selectable by scheduled time, guard, route or status, shall be included in the application.

b. The system shall provide the capability to query and display the status of a tour in progress, showing the location of the guard at any given time during the tour, both by text and map display.

c. Deviations from the tour schedule shall be capable of generating an alarm.

d. The system shall also provide the capability to shunt and unshunt monitor points, via time schedule, in order to allow the guard tour to proceed from one station to another without restriction. Readers, as well as monitor points, shall be allowed as guard tour points.]

5. [**Time & Attendance** (optional module):

a. **General:** The system shall provide a real-time personnel time data collection system with capability to:

1) Automate the capture of hours worked

2) Provide error free input data to a payroll system

3) Provide timely and accurate time reporting

b. **Functionality:**

1) Dual functionality readers that function both as access control readers and as time and attendance clock stations, with a simultaneous read for both activities.

2) Single or dual directional stations with either one reader for clock in/out or both clock in and clock out readers.

3) Automatic transaction logging to the time and attendance database. The logs shall include card holder id, no less than 6 user definable fields, clock in/out date and time.

4) Time transaction editing capability to ensure that data is accurate and complete prior to transmittal to an ancillary database.

5) Time transaction reporting to provide a means of verifying the accuracy of any transactions to be exported to a payroll system.]

6. [**Electronic Visitor Directory** (optional module):

a. **General:** The system shall provide an Electronic Visitor Directory option by which to process and monitor visitors to a facility. This module shall provide the capability of storing both permanent and current information for each visitor, as well as flexible reporting and badge printing capabilities.

b. **Database:** A permanent database entry shall exist for each visitor, that can be retrieved, modified and expanded with each ensuing visit, and transferred to the correct files for badge creation, storage and reporting.

c. **Reporting:** Visitor reporting shall be selectable according to specific search criteria.

d. **Pre-registration:** The system shall also provide the capability for pre-registration and advance preparation of visitor badges in order to facilitate the visitor registration process.]

7. [**Remote Dial-up Interface** (optional hardware):

a. **General:**

1) The system shall provide dial-up capability through an intelligent link between Host and multiple Controllers, via dial-up phone lines.

2) A microprocessor-based hardware platform in conjunction with application software shall provide remote dial-up support for no less than 3 Controllers.

b. **Functions:** The functionality of a remote dial-up interface shall include the following:

1) Automatic, high-speed download of data from Host to the Controller, thereby eliminating data integrity problems and the need for human intervention between the two device types.

2) Error free download of data through a communications protocol to provide error detection and acknowledgment of each transaction as it is received by Host computer.

3) Automatic re-transmission of downloaded data upon detection of an error through a database verification and memory check procedure.

4) Buffer storage capacity of no less than 6,000 transactions, with an automatic dial-out upon a pre-defined threshold.

5) Immediate call in, to Host computer, of alarms based upon a user-definable table of alarm conditions.

6) Redundant communications path with no less than 3 programmable, alternative phone numbers to the RDI unit, which shall be used in the event of a communications failure to Host computer. Upon dial-out of an alternative phone number, the alarm condition or transaction buffer shall be routed to an optional computer, thereby triggering a report of the communications failure to the primary computer.]

8. [**Parking/ Revenue Control** (optional module):

a. **General:** The system shall provide the capability to control access to, and the revenue generated by, a parking facility. Through integration of cardholder access control with the cashiering function required for transient parkers, the system shall provide total control of a parking facility by tracking entry and egress of any type.

b. **Functions:** The parking control system shall encompass both the control of cardholder parking and the control of transient parking by providing the following functionality:

1) Keyholder Parking Control:

(i) The same system that controls access to any facility shall control access to parking, thereby optimizing the use of a single access card per cardholder.

(ii) The capability shall be provided to define parking access privileges by day of week, time of day, and card reader.

(iii) Anti-passback shall also be supported.

(iv) Nesting control shall be provided in order to monitor and track a cardholder who has parked outside of a designated area. The system shall provide the capability for a reader, or series of readers, to be defined for the sole purpose of allowing access to an inner, or nested, parking area. A flag shall be triggered whenever a reader in the "nesting" path is accessed. Upon accessing the reader in the designated area, the flags shall be removed. However, if the designated reader is not accessed, an alert shall generated and a permanent transaction shall be logged for reporting.

(v) The system shall provide the capability to maintain a tenant file for billing and revenue control in association with parking control, and to monitor and track the parking population on demand.

2) Transient Parking Control:

(i) The system shall provide support for interface with standard parking ticket spitters, cash ticket processing, validated ticket processing, online ticket validation, no ticket processing, and daily cash control through report generation.

(ii) NOTE: The specifier should carefully select the portions of this section that fit the intended application. Budgetary considerations are very important in selecting these features since many of them require additional hardware and/or software.]

.4 COMPONENT DEFINITION

A. Hewlett-Packard computers are required for this system. Seven models may be implemented depending on the nature of the system integrator's design. The four standard platforms designated for the seven models are defined below, each configuration specifying minimum requirements:

1. **SE 6030/40/50 System Hardware and Software:**

a. Manufacturer/Model: Hewlett-Packard SM3 Series.

b. Microprocessor: Pentium, 32-bit minimum.

c. Processing speed: 50 mhZ minimum.

d. Random Access Memory: 16 MB minimum.

e. Monitor: 256 Color, Super Video Graphics Array (SVGA) standard 110/220v selectable UL Listed, or better.

f. Mass Storage: 540 MB fixed disk drive.

g. Backup Media: 150 MB streaming tape drive.

h. I/O Ports:

1) Mouse port.

2) 1 parallel port.

3) 9 RS232 serial ports.

4) Integrated LAN.

i. Input media: 1.44 MB 3.5" diskette drive.

j. Keyboards:

1) 101 Key IBM PC/AT Enhanced Keyboard Format.

2) Foreign language keyboards are available.

k. Printer: Hewlett Packard LaserJet 5 Report Printer, LaserJet 5L Printer, Serial Log Printer.

l. Communications: RS-232.

m. Operating System: SCO UNIX System V, with SCO Color Graphics Interface.

n. Database Management System: UNIFY Accell SQL.

o. Advanced Visual Report Writer: Yes.

p. Other:

1) Tilt/swivel base.

2) UL and FCC approved.

3) Made in the USA.

2. **SE 6100 or LC/1, or RLC/1 System Hardware and Software:**
   a. Manufacturer/Model: Hewlett-Packard SM3 Series.
   b. Microprocessor: Pentium, 32-bit minimum.
   c. Processing speed: 77 MHz.
   d. Random Access Memory: 24 MB minimum.
   e. Monitor: 256 Color, Super Video Graphics Array (SVGA) standard 110/220v selectable UL Listed, or better.
   f. Mass Storage: 540 MB fixed disk drive.
   g. Backup Media: 150 MB streaming tape drive.
   h. I/O Ports:
      1) Mouse port.
      2) 1-parallel port.
      3) 9-RS232 serial ports.
      4) Integrated LAN.
   i. Input media: 1.44 MB 3.5" diskette drive.
   j. Keyboards:
      1) 101 Key IBM PC/AT Enhanced Keyboard Format.
      2) Foreign language keyboards are available.
   k. Printer: Hewlett Packard LaserJet 5 Report Printer, LaserJet 5L Printer, Serial Log Printer.
   l. Communications: RS-232.
   m. Operating System: SCO UNIX System V, with SCO Color Graphics Interface.
   n. Database Management System: UNIFY Accell SQL.
   o. Advanced Visual Report Writer: Yes.
   p. Other:
      1) Tilt/swivel base.
      2) UL and FCC approved.
      3) Made in the USA.
3. **SE 6200 or LC/2 or RLC/2 System Hardware and Software:**
   a. Manufacturer/Model: Hewlett-Packard SM3 Series.
   b. Microprocessor: Pentium, 32-bit.
   c. Processing speed: 90 MHz.
   d. Random Access Memory: 32 MB (expandable to 64 MB).
   e. Monitor: 256 Color, Super Video Graphics Array (SVGA) standard 110/220v selectable UL Listed, or better.
   f. Mass Storage: 840 MB fixed disk drive.
   g. Backup Media: 150 MB streaming tape drive.
   h. I/O Ports:
      1) Mouse port.
      2) 1-parallel port.
      3) 17-RS232 serial ports.
      4) Integrated LAN.

i. Input media: 1.44 MB 3.5" diskette drive.

j. Keyboards:

1) 101 Key IBM PC/AT Enhanced Keyboard Format.

2) Foreign language keyboards are available.

k. Printer: Hewlett Packard LaserJet 5 Report Printer, LaserJet 5L Printer, Serial Log Printer.

l. Communications: RS-232.

m. Operating System: SCO UNIX System V, with SCO Color Graphics Interface.

n. Database Management System: UNIFY Accell SQL.

o. Advanced Visual Report Writer: Yes.

p. Other:

1) Tilt/swivel base.

2) UL and FCC approved.

3) Made in the USA.

4. **SE 6300 or LC/3 or RLC/3 System Hardware and Software:**

a. Manufacturer/Model: Hewlett-Packard SM3 Series.

b. Microprocessor: Pentium, 32-bit.

c. Processing speed: 120 MHz.

d. Random Access Memory: 32 MB (expandable to 64 MB).

e. Monitor: 256 Color, Super Video Graphics Array (SVGA) standard 110/220v selectable UL Listed, or better.

f. Mass Storage: 1 GB SCSI-2 fixed disk drive.

g. Backup Media: 150 MB streaming tape drive.

h. I/O Ports:

1) mouse port.

2) 1-parallel port.

3) 33-RS232 serial ports.

4) Integrated LAN.

i. Input media: 1.44 MB 3.5" diskette drive.

j. Keyboards:

1) 101 Key IBM PC/AT Enhanced Keyboard Format.

2) Foreign language keyboards are available.

k. Printer: Hewlett Packard LaserJet 5 Report Printer, LaserJet 5L Printer, Serial Log Printer.

l. Communications: RS-232.

m. Operating System: SCO UNIX System V, with SCO Color Graphics Interface.

n. Database Management System: UNIFY Accell SQL.

o. Advanced Visual Report Writer: Yes.

p. Other:

1) Tilt/swivel base.

2) UL and FCC approved.

3) Made in the USA.

5. **Accessories:**

a. **Optional Peripheral Devices:**

1) Printer:

(i) Hewlett Packard LaserJet 5 Report Printer.

(ii) LaserJet 5L Report Printer.

(iii) Okidata Serial Log Printer.

(iv) Okidata Parallel Log Printer.

2) **Terminal:**

(i) Hewlett Packard Monochrome Terminal or Color Graphics Terminal.

(ii) Terminal emulation software

(iii) 2-button serial mouse (required for real-time maps)

b. **Optional ancillary equipment:**

1) **Communication Modems:**

(i) Direct Connection: Short distance (max. two miles point-to-point on 22-AWG twisted pair at 9600 baud.) Uses Black Box short haul modems, ME800A.

(ii) Dial-Up Connection: Telebit T-1000 (US only) modems: The Telebit modems support dial-up capability at 9600 baud.

(iii) Conversion modems from 20 ma to RS-232: Westinghouse Security Electronics CI-1 or CI-8.

2) **Power Management:**

(i) UPS: Provides continuous power, without interruption, should primary power source be interrupted. Provides 1 hour or more continuous DC power, depending on configuration.

PART III EXECUTION

.1 FIELD QUALITY CONTROL

A. **Tests:**

1. The selected system integrator shall supply a proposed acceptance test procedure.
2. Testing the system shall be the sole responsibility of the system integrator.
3. Communications tests:

a. Controllers to Host, Local Controller or Remote Location Controller.

b. Local Controllers or Remote Location Controllers to Host.

c. Additional terminals or printers attached to Host or controller.

d. Remote dial-up support.

B. **Inspection:**

1. The selected system integrator shall provide, on the job site, a factory-trained technician to assist, advise or manage installing personnel.
2. All final connections shall be made under the direct supervision of the system integrator.

C. **Field Service:**

1. A systems integrator, authorized by the manufacturer, shall provide first line support for both the hardware and software properties of the selected system.
2. The system integrator shall in turn be provided second line support directly from the manufacturer, or manufacturer's OEM, for all component and computer hardware, and all operating and application software which comprise the complete system.
3. The systems integrator shall determine and report all problems to the manufacturers' customer service departments.

4. Support shall be available to the integrator via the following methods:
    a. Phone inquiries.
    b. Direct dial-in to the customer system for remote system troubleshooting by a qualified Field Service Engineer.
    c. On-site visits if required, upon approval by the manufacturer's Customer Service Manager.
5. Manufacturer shall provide reliable field service support for the computer hardware utilizing Hewlett Packard service.
6. A complete Hewlett-Packard On-site Warranty/Service Agreement is provided with each standard system utilizing Hewlett-Packard computer hardware. This agreement shall provide complete on-site service with a one-day response time guaranteed, from Monday through Friday, 8:00 am to 5:00 p.m. from a local Hewlett Packard Service Center.
7. Extended and peripheral service and maintenance agreements shall be available for purchase by the customer.

D. **On-Site commissioning and/or training:**

1. The manufacturer shall provide direct participation in the On-Site Commissioning (OSC) activity of new systems, in conjunction with the systems integrator.
2. The OSC shall provide the systems integrator with the manufacturer's expertise on installing, configuring and commissioning the system to the customer's specific requirements; and to provide on-site training on system operation and administration.
3. On-site factory training shall be available for system administrators, operators and other qualified personnel.
4. The OSC shall include the following:
    a. Hardware set-up and test.
    b. Communication configuration and test.
    c. Preventative maintenance and troubleshooting training for the systems integrator.
    d. End-user training.
    e. Database configuration and build assistance.

.2 SCHEDULES

A. **System Integrator Assisted Preparation:**

1. Data Requirements.
2. Operators & privileges.
3. Access Hardware.
4. Sensors.
5. Monitor Points.
6. Keyholders.
7. Keyholders security codes.
8. Maps.
9. Prepare room for system installation.
10. Receive equipment.

B. **System Installation:**

1. Install security management hardware.
2. Factory and dealer On-Site Commissioning.
3. Initial startup and verification.
4. Data Entry.
5. Data Entry listing & verification.

C. **Verify Installation:**

1. Connect access control hardware to security management system.
2. Download data and verify correct operation.
3. Testing total access and management system.
4. Sample Reports.
5. Daily Operation and Monitoring.
6. Dealer deliver “as built” drawings.

PART IV APPENDIX

.1 REMOTE DIAL-UP INTERFACE: MODEL RDI

A. **SE 6000 Remote Dial-up Interface:** This interface is designed for the SE 800 Series products.

1. **Each RDI Unit supports 3 Controllers** which includes :

a. SE 6000 remote dial-up interface software:

1) Access control and alarm monitoring capability.

2) 8 door & 32 monitor point capability.

3) Dial-up capability to SE 6100/6200/6300 systems.

b. SE 6000 remote dial-up interface hardware:

1) Intel 286 microprocessor.

2) Dial-up remote support modem: Telebit or Hayes compatible modem, 1200 to 9600 baud support.

2. **Optional Monitors:**

a. Monochrome (ASCII text):

1) Hewlett Packard.

2) Monochrome ASCII screen (80 characters by 24 lines).

3) Keyboard.

4) Auxiliary printer port.

b. Color Graphics or X-Terminal:

1) Hewlett Packard SM3 PC.

2) Intel 486 25 MHZ processor.

3) 1 MB memory.

4) 1.44 MB 3.25" floppy disk drive.

5) 340 MB hard disk drive.

6) SVGA color monitor and adapter.

7) Hewlett Packard mouse.

8) MS DOS 3.3

9) Reflection Terminal Emulation software, which provides terminal emulation on a PC using DOS for full color graphics, or;

10) X-Terminal with Windows.

11) Functions as a color graphics terminal under control of UNIX.

.2 DATABASE CAPACITIES

A. **6030/40/50 System Database Capacities:**

6030/40/50 HARDWARE / DATA	STANDARD	MAXIMUM
User Terminals	1	4
Keyholders	5,000	8,000
Access Codes	1,000	2,000
Read/Time Code Combinations	5,000	8,000
Access Groups	500	1,000
Access Code Combinations	50,000	100,000
Access Code/Group Combinations	10,000	16,000
Operator Passwords	100	1,000
Time Codes	100	1,000
Holidays	50	1,000
Floor Plan Maps	100	1,000
Online Transaction Storage	100,000	250,000
Off-line Transaction Storage	Unlimited	Unlimited
Local Controllers (LCs)	redundancy only	redundancy only
Remote Location Controllers (RLCs)	0	0
Remote Dial-Up Interfaces (RDIs)	0	0

	Central	Distributed
Controllers	4/8	4/16
Sensors	32/64	32/128
Sensors with Keypads	32/64	32/128
Monitor Points	128/512	128/512
Output Relays	64/128	64/256

Note: Maximum capacities require additional hardware or software.

B. **6100 System Database Capacities:**

6100 HARDWARE / DATA	STANDARD	MAXIMUM
User Terminals	1	4
Keyholders	20,000	64,000
Access Codes	2,000	8,000
Read/Time Code Combinations	8,000	64,000
Access Groups	1,000	16,000
Access Code Combinations	100,000	400,000
Access Code/Group Combinations	16,000	128,000
Operator Passwords	100	1,000
Time Codes	100	1,000
Holidays	50	1,000
Floor Plan Maps	150	1,000
Online Transaction Storage	250,000	800,000
Off-line Transaction Storage	Unlimited	Unlimited
Local Controllers (Lcs)	4	4
Remote Location Controllers (RLCs)	16	16
Remote Dial-Up Interfaces (RDIs)	64	64

	Central	Distributed
Controllers	16	32
Sensors	128	256
Sensors with Keypads	64	256
Monitor Points	512	1,024
Output Relays	256	512

Note: Maximum capacities require additional hardware or software.

C. **6200 Systems Database Capacities:**

6200 HARDWARE / DATA	STANDARD	MAXIMUM
User Terminals	1	8
Keyholders	40,000	128,000
Access Codes	5,000	32,000
Read/Time Code Combinations	20,000	128,000
Access Groups	8,000	32,000
Access Code Combinations	200,000	800,000
Access Code/Group Combinations	40,000	256,000
Operator Passwords	100	1,000
Time Codes	100	1,000
Holidays	50	1,000
Floor Plan Maps	150	1,000
Online Transaction Storage	500,000	2,000,000
Off-line Transaction Storage	Unlimited	Unlimited
Local Controllers (Lcs)	8	8
Remote Location Controllers (RLCs)	32	32
Remote Dial-Up Interfaces (RDIs)	128	128

	Central	Distributed
Controllers	32	64
Sensors	256	512
Sensors with Keypads	256	512
Monitor Points	1,024	2,048
Output Relays	512	1,024

Note: Maximum capacities require additional hardware or software.

D. **6300 System Database Capacities:**

6300 HARDWARE / DATA	STANDARD	MAXIMUM
User Terminals	1	12
Keyholders	64,000	128,000
Access Codes	10,000	32,000
Read/Time Code Combinations	40,000	128,000
Access Groups	16,000	32,000
Access Code Combinations	400,000	800,000
Access Code/Group Combinations	80,000	256,000
Operator Passwords	100	1,000
Time Codes	100	1,000
Holidays	50	1,000
Floor Plan Maps	150	1,000
Online Transaction Storage	1,000,000	2,000,000
Off-line Transaction Storage	Unlimited	Unlimited
Local Controllers (LCs)	16	16
Remote Location Controllers (RLCs)	64	64
Remote Dial-Up Interfaces (RDIs)	256	256

	Central	Distributed
Controllers	64	128
Sensors	512	1,024
Sensors with Keypads	512	1,024
Monitor Points	2,048	4,096
Output Relays	1,024	2,048

Note: Maximum capacities require additional hardware or software.

E. **LC / RLC System Database Capacities:**

HARDWARE / DATA	CENTRAL	DISTRIBUTED
User Terminals	1	2
Controllers	16	32
Sensors	128	256
Sensors with Keypads	64	0
Monitor Points	512	1,024
Output Relays	256	512

F. **LC1 / RLC1 System Database Capacities:**

HARDWARE/DATA	CENTRAL	DISTRIBUTED
User Terminals	1	2
Controllers	32	64
Sensors	256	512
Sensors with Keypads	256	512
Monitor Points	1,024	2,048
Output Relays	512	1,024

G. **LC2 / RLC2 System Database Capcities:**

HARDWARE/DATA	CENTRAL	DISTRIBUTED
User Terminals	1	2
Controllers	64	128
Sensors	512	1,024
Sensors with Keypads	512	1,024
Monitor Points	2,048	4,096
Output Relays	1,024	2,048

H. **LC2 / RLC2 System Database Capacities:**

HARDWARE/DATA	CENTRAL	DISTRIBUTED
User Terminals	1	2
Controllers	128	256
Sensors	1,024	2,048
Sensors with Keypads	1,024	2,048
Monitor Points	4,096	8,192
Output Relays	2,048	4,096

Note: Maximum capacities require additional hardware or software.